International Journal of Research in Science & Technology
Volume 2 | Issue 5 | May 2015 | ISSN: 2349-0845

An Efficient User Privacy and Protecting Location Content in Location Based Service

D. Linta Nayagi[1] and V. Gunalan[2]

[1]PG Student, Department of CSE, Bharathiyar College of Engineering & Technology, Thiruvettakudy Karaikal, Pondicherry, India
[2]Assistant Professor, Department of CSE, Bharathiyar College of Engineering & Technology, Thiruvettakudy Karaikal, Pondicherry, India

Article Info

Article history:

Received on 16th April 2015
Accepted on 21st April 2015
Published on 27th April 2015

Keyword:

Location based query, private information retrieval, oblivious transfer, homomorphic data.

ABSTRACT

In location-based query a user wants to query a database of location data, known as Points Of Interest (POIs), and does not want to reveal his/her location to the server due to privacy concerns; (ii) the owner of the location data, that is, the location server, do Abstract: Nowadays, it is very easy for a person to learn his/her location with the help of a Global Positioning System (GPS) enabled device. A location s not want to simply distribute its data to all users. The location server desires to have some control over its data, since the data is its asset. A major enhancement upon previous solutions by introducing a two stage approach, the first step is based on Oblivious Transfer using homomorphic encryption and the second step is based on Private Information Retrieval, to achieve a secure solution for both parties. Introduce a security model and analyse the security in the context of our protocol. To highlight a security weakness of our previous work and present a solution using efficient homomorphic system.

Corresponding Author:

D. Linta Nayagi
PG Student, Department of CSE,
Bharathiyar College of Engineering & Technology,
Thiruvettakudy
Karaikal, Pondicherry, India.
Email ID: lins.lntng@gmail.com

I. INTRODUCTION

Location-based services (LBS) are services that exploit knowledge about an information device is located. It applies the field of data mining and information security. Gathereing the information from the system available through an interface to various government and private entities such as fire departments,thepolice,ambulances,hotels,transportation,customs,etc. Developing an software application (app) for various mobile platforms/devices including iPhones, Androids and BlackBerry's. This will utilize the data to provide a privacy of location based services (LBS).

To protect user privacy in location based queries search to obtain requiring privacy and usability in a user controllable manner. Such location can be represented in a variety of ways and depending on the context LBS can utilize several techniques for knowing an information device is geographically located.

II. PROBLEM STATEMENT

The privacy-aware LBS is to protect a user's private information from potentially malicious servers while responding to his queries .To achieve location privacy, user location and identity information for identifying of query results for both on the server and query evaluation. PIR to achieve such strong measures of privacy by placing trust on a secure coprocessor residing at the server side which is in charge of initiating PIR requests to the server and privately evaluating user queries .

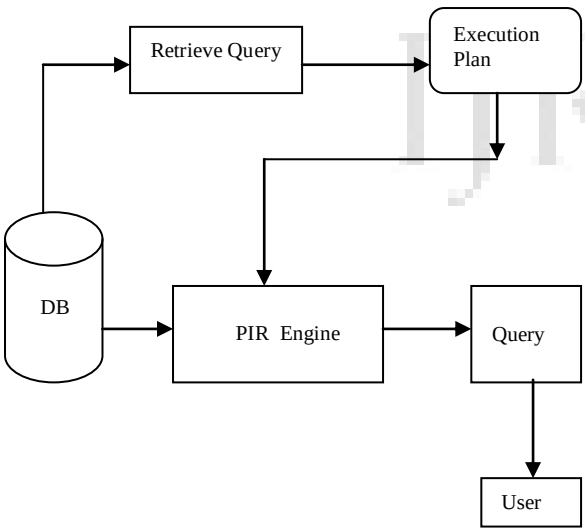

Figure 1: PIR Query Execution

Two components in Query Execution first one is PIR functionality ,and second is the query plan .The query plan ensures that every query retrieves the same number of blocks during its execution.

A. System Model

The system model consists of three types of entities first set of users to access location data and a service provider SP, and a location server, the SP and LS will compose a server, that will serve both functions. The user does not need to be concerned with the communication. The user would communicate a search keyword to the provider, and retrieve a ranked list of records matching the search term.

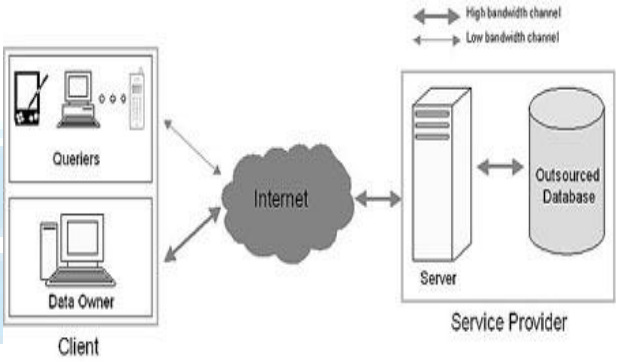

Figure 2: System Model

III. PROPOSED SYSTEM

We design an modal for location based queries with homomorphic encryption that have major performance improvements with respect to the approach. The user privately determines his/her location within a grid in encryption way. This provides protection for both the user and the server. The user is protected because the server is unable to determine his/her location. Similarly, the server's data is protected since a malicious user can only decrypt the block of data obtained by PIR with the encryption key acquired in the previous stage. The users in our model use some location-based service provided by the location server LS. For example, what is the nearest hospital or hotel.

We obtaining Location based information is extracted from the spatial database. User are responsible for retrieving the information through the query's derived from the location server. And updating the query and displaying search results are handled by the search data, are handled by the location server . Protecting sensitive information about an individual user's location, at the same time as providing useful location-based services to that user.Information can be exchanged between the user and the service provider to allow query results across a geographic area. Results indicate the possibility of large default privacy regions (areas of no change in result set) according to each latitude and longitude pairs.

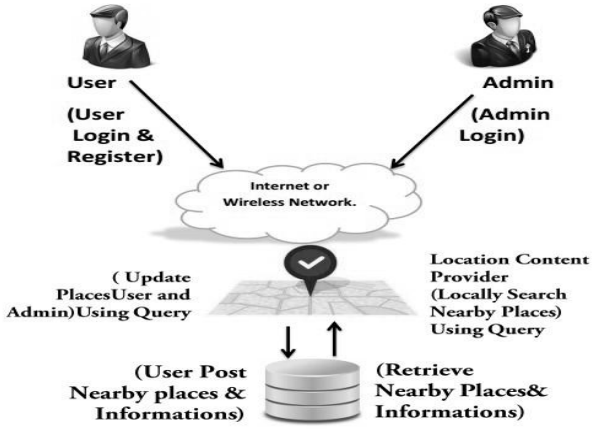

Figure 3: System Architecture Diagram

To establish and maintain the communication between the location server and the user for accessing location based information with a secure manner.

A. Techniques

i. Private Information Retrieval

In the PIR protocol allows a user to retrieve an information from a location server of a database without revealing which information is retrieve. The user can initiate a private information retrieval protocol with the location server to acquire the encrypted POI data. The user information theoretic privacy for their query in a location server . There are two ways to address the problem: one is to mae the server computationally bounded and the each having a copy of the database. PIR protocol require an amount of communication that is least the size of the database n. PIR protocols tolerant of non-responsive or malicious server are called robust or Byzantine robust respectively.

The basic motivation for Private Information Retrieval is a two-party protocols in which one of the parties (the sender) owns a database, and the other part(the receiver) wants to query it with certain privacy restrictions. As a result of the protocol, if the receiver wants the i-th value in the database he must learn the i-th entry, but the sender must learn nothing about i so privacy is theoretically preserved.

ii. oblivious Transfer Protocol

An oblivious transfer protocol is a type of protocol in which a sender transfer one of potentially many pieces of information to a receiver , but remains oblivious as to what piece has been transferred. In the receive retrieves an element chosen by from the database. The Sender obtains no knowledge about which information is retrieved.

iii. Homomorphic Encryption

We design a novel for encryption as Homomorphic Encryption which allows specific types of computations to be carried out on ciphertext and generate an encrypted result which, decrypted and matches the result of operations performed on the plaintext. It would allow the chaining together of different services without exposing the data of location server.

This system supports both latitude and longitude is fully homomorphic encryption (FHE) and more powerful. Evaluating an encryption of their input to produce an encryption of their output . Homomorphic encryption performes an encrypted data with each latitude and longitude pairs. The transformation of one data set into another while preserving relationships between elements in both sets.

Homomorphic Encryption can be carried out as fellowing steps.

- Ciphertext
- Generating encrypted result
- Decryt
- Matches the results of operations performed on the plaintext.

IV. Related Work

Gabriel Ghinit proposed an hybrid approach, outlined in the LS, which determines a set of user and the LS engage in a novel cryptographic protocol that privately determines the location information .Then a PIR round to retrieve the content. The amount of protection offered to the database by the hybrid method, in comparison with location cloaking (label CR-only) and the pure-PIR technique (label PIR-only), for varying CR size. The PIR-only method does not use CRs, and always discloses approximately 250 POI (square root of database cardinality).**Ali Khoshgozaran** proposed an privacy metrics, the adversary and the information leak model and use them throughout to evaluate the privacy. The key idea behind our approach is to use PIR to privately query the index structures stored at the untrusted server to perform spatial queries. these algorithms are executed depends on the underlying PIR protocol employed. To achieve such strong measures of privacy by placing trust on a secure coprocessor residing at the server side which is in charge of initiating PIR requests to the server and privately evaluating user queries.

Jun Pang proposed an mechanism to protect users' location and query privacy is spatial.As more user information becomes available with the fast growth of Internet applications ,e.g., social networks, attackers have the ability to construct users' personal profiles. This gives rise to new challenges and reconsideration of the existing privacy metrics, such as k-anonymity. we propose an new metrics to measure users' query privacy taking into account user profiles. To satisfying users' privacy requirements expressed in these metrics. Location-based queries lead to privacy concerns especially in cases when LBSPs are not trusted. Tan et al. define

information leakage to measure the amount of revealed location information in spatial cloaking, which quantifies the balance between privacy and performance introduce the concept of location diversity to ensure generalised regions to contain at least ` semantic locations (e.g., schools, hospitals).

V. Conclusion

In this work, we proposed an efficient location based query involves a private information retrieval interaction that retrieves the record with high communication efficiency using Homomorphic Encryption which allows specific types of computations to be carried out on ciphertext and generate an encrypted result which, decrypted and matches the result of operations performed on the plaintext. It would allow the chaining together of different services without exposing the data of location server. These updates can happen in the background, and the query processor can have access to the updated database.Using the prototypical example of a local search application, the information that can be exchanged between the user and the provider to enable a privacy-supportive LBS. Further to this work, the privacy of user information who try to retrieve the data can be maintained by applying the private information retrieval and the user may post an query using both latitude and longitude pairs..

Acknowledgment

This work was supported in part by ARC DiscoveryProject (DP0988411) “Private Data Warehouse Query” andin part by NSF award (1016722) “TC: Small:Collaborative: Protocols for Privacy-Preserving Scalable Record for accessing the tagged posts by latitude and longitude pairsof given record.”.

References

[1] C. Bettini, X. Wang, and S. Jajodia, “Protecting privacy againstlocation-basedpersonal identification,” in Proc.2nd VDLB Int.Conf. SDM, W. Jonker and M. Petkovic, Eds., Trondheim, Norway. 2005, pp. 185–199, LNC3674.

[2] X. Chen and J. Pang, “Measuring query privacy in location-based services,” in Proc. 2nd ACM CODASPY, San Antonio, TX, USA, 2012, pp. 49–60

[3] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” IEEE Trans. Inform. Theory, vol. 31, no. 4, pp. 469–472, Jul. 1985.

[4] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, “A hybrid technique for private location-based queries with database protection,” in Proc. Adv. Spatial Temporal Databases.

[5] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, “Private queries in location based services: Anonymizers are not necessary,” in Proc. ACM SIGMOD,Vancouver, BC, Canada, 2008, pp. 121–132.

[6] M. Gruteser and D. Grunwald, “Anonymous usage of locationbased services through spatial and temporal cloaking,” in Proc. 1st Int. Conf. MobiSys, 2003, pp. 31–42.

[7] B. Hoh and M. Gruteser, “Protecting location privacy through path confusion,” in Proc.1st Int. Conf. SecureComm, 2005, pp. 194–205.

[8] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, “Preventing location-based .

[9] identity inference in anonymous spatial queries,” IEEE Trans. Knowl. Data Eng., vol. 19, no. 12, pp. 1719–1733, Dec. 2007.

[10] M. Duckham and L. Kulik, “A formal model of obfuscation and negotiation for location privacy,” in Proc. 3rd Int. Conf. Pervasive Comput., H. Gellersen, R. Want, and A. Schmidt,Eds., 2005, pp. 243–251, LNCS 3468.

[11] M. Bellare and S. Micali, “Non-interactive oblivious transfer and applications,” in Proc. CRYPTO, 1990, pp. 547–557.

[12] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, “Preventing location-based.

[13] identity inference in anonymous spatial queries,” IEEE Trans. Knowl. Data Eng., vol. 19,

[14] H. Kido, Y. Yanagisawa, and T. Satoh, “An anonymous communication technique using dummies for location-based services,” in Proc. Int. Conf. ICPS, 2005, pp. 88–97.

[15] M. Bellare and S. Micali, “Non-interactive oblivious transfer and applications,” in Proc.